PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-147984
(43)Date of publication of application : 29.05.2001

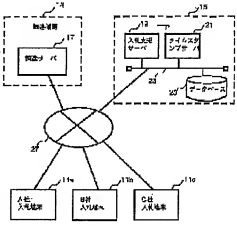
(51)Int.Cl. G06F 19/00
G09C 1/00

(21)Application number : 11-331274
(22)Date of filing : 22.11.1999

(71)Applicant : NTT DATA CORP
(72)Inventor : MOTONAGA KIMIAKI

(54) SYSTEM AND METHOD FOR ELECTRONIC VOTING

(57)Abstract:
PROBLEM TO BE SOLVED: To enable high-reliability electronic tendering, with which illegality can be surely verified.
SOLUTION: Each of tendering terminals 11a, 11b and 11c generates the hash value of a tender document, enciphers the document with its own secret key and transmits the enciphered hash document to a TTP 15. The TTP prepares an SHV certificate concerning each of enciphered hash documents and calculates an SHV every second. The TTP discloses the SHV of every second of each of enciphered hash documents and each of enciphered hash documents, to which the SHV certificate is attached, on the Internet 27. Before tendering to a procurement institution 13, each of tendering terminals downloads the enciphered hash document with SHV certificate. The procurement institution discloses a tender document 107 of a successful bidder company. Each of tendering terminal downloads the tender document of the successful bidder company, takes the hash thereof, deciphers the hash value after successful bid and the enciphered hash document of the successful bidder company, compares the deciphered value with the hash value before the successful bid and when these values are not coincident, it is judged the tender document of the successful bid is illegally revised.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号
特開2001－147984
（P2001－147984A）
(43)公開日　平成13年5月29日(2001.5.29)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　19/00		Ｇ０９Ｃ　1/00	６４０Ｚ	５Ｂ０４９
Ｇ０９Ｃ　1/00	６４０	Ｇ０６Ｆ　15/28	Ｂ	５Ｊ１０４
				９Ａ００１

審査請求　有　　請求項の数23　ＯＬ　（全 14 頁）

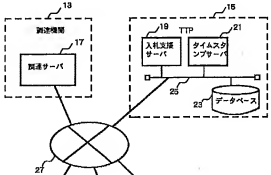
(21)出願番号　特願平11－331274
(22)出願日　平成11年11月22日(1999.11.22)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　木永　公章
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095371
弁理士　上村　輝之

Ｆターム(参考)　5B049 AA05 BB36 CC01 CC31 EE03
EE05 GG04 GG07 GG10
5J104 AA08 LA03 LA05 MA02 NA12
PA07 PA17
9A001 EE03 JJ25 JJ27 JJ71 LL03

(54)【発明の名称】　電子投票方式、及び方法

(57)【要約】　（修正有）
【課題】　不正を確実に検証できる信頼性高い電子入札。
【解決手段】　各入札端末１１ａ、１１ｂ、１１ｃは、入札文書のハッシュ値を生成してそれを自分の秘密鍵で暗号化し、その暗号化ハッシュ文書をＴＴＰ１５に送信する。ＴＴＰは、各暗号化ハッシュ文書について、ＳＨＶ証明書を作成し、且つ、毎秒ＳＨＶを算出する。ＴＴＰは、各暗号化ハッシュ文書の毎秒のＳＨＶと、ＳＨＶ証明書を添付した各暗号化ハッシュ文書を、インターネット２７上に公開する。各入札端末は、調達機関１３に入札する前に、ＳＨＶ証明書付きの暗号化ハッシュ文書をダウンロードしておく。調達機関は、落札社の入札文書１０７を公開する。各入札端末は、落札社の入札文書をダウンロードして、そのハッシュをとり、開札後のハッシュ値と、落札社の暗号化ハッシュ文書を復号化して開札前のハッシュ値とを比較し、それらが一致していなければ、落札された入札文書は不正に改竄されたと判断する。



1

【特許請求の範囲】

【請求項１】　投票書類の内容を記録した投票書類データを生成する１又は複数の情報処理装置と、信頼される第三者機関と、前記投票書類データが調達される機関とを備え、

前記第三者機関が、暗号化された前記投票書類データの各々を公開するための手段を備え、

前記調達機関が、前記調達された投票書類データの各々に基づく開票の結果を示すデータを公開するための手段を備え、

前記１又は複数の情報処理装置が、

前記投票書類データを暗号化してそれを前記第三者機関に送るための第１の送り手段と、

前記投票書類データを前記調達機関に送るための第２の送り手段と、

前記公開された暗号化投票書類データを入手するための第１の入手手段と、

前記公開された開票結果データを入手するための第２の入手手段と、

不正の有無を検知するために、前記開票結果データと前記暗号化投票書類データとを比較する手段とを備える電子投票方式。

【請求項２】　前記第三者機関において、

前記暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成する手段が更に備えられ、

前記公開するための手段が、前記生成した証明書の各々を、それらに対応する前記暗号化投票書類データに添付して公開するようにし、

前記１又は複数の情報処理装置において、

前記第１の入手手段が、前記公開された前記暗号化投票書類データと共に前記証明書を入手し、

前記比較する手段が、不正の有無を検知するために、前記開票の日時と、前記入手した証明書に付けられた日時とを更に比較する請求項１記載の電子投票方式。

【請求項３】　前記１又は複数の情報処理装置において、

前記投票書類データの特徴データを生成する手段が更に備えられ、

前記第１の送り手段が、前記特徴データを暗号化したものを前記第三者機関に送るようにし、

前記第三者機関において、

前記公開するための手段が、前記暗号化特徴データの各々を公開するようにし、

前記１又は複数の情報処理装置において、

前記第１の入手手段が、前記公開された暗号化特徴データを入手し、

前記比較する手段が、不正の有無を検知するために、前記開票結果データの特徴データを生成し、その開票結果データの特徴データと、前記入手した暗号化特徴データとを比較する請求項１記載の電子投票方式。

2

【請求項４】　前記第三者機関において、

前記証明書に付けられた日時以後、任意の時に前記暗号化特徴データの別特徴データを生成する手段と、

前記任意の時に生成した別特徴データを公開するための手段が更に備えられ、

前記証明書を生成する手段が、前記暗号化特徴データの各々に対し、前記暗号化特徴データの別特徴データを生成した日時と、その日時に生成した別特徴データを前記暗号化特徴データを用いて生成するための方法とを記録した証明書を生成し、

前記１又は複数の情報処理装置において、

前記比較する手段が、不正の有無を検知するために、前記公開された別特徴データから、前記比較の対象の特徴データに対応する証明書に記録された生成日時のときの別特徴データを入手し、且つ、前記比較対象の特徴データとそれの証明書に記録された前記生成方法とに基づいて前記比較対象の特徴データの別特徴データを生成し、その生成した別特徴データと前記入手した別特徴データとを比較する請求項２又は３記載の電子投票方式。

【請求項５】　前記特徴データ又は前記別特徴データは、ハッシュ値である請求項３又は４記載の電子投票方式。

【請求項６】　前記１又は複数の情報処理装置において、前記第２の送り手段が、前記入手した証明書のうち、前記生成した投票書類データに対応する証明書をその投票書類データに添付して、それを前記調達機関に送るようにする請求項２乃至請求項５のいずれか一項記載の電子投票方式。

【請求項７】　前記開票の後に、前記投票の参加者から不正があった旨が報知されたときは、

前記１又は複数の情報処理装置において、

前記第１又は第２の入手手段が、前記報知を行なった投票参加者が保持する投票書類データを入手するようにし、

前記比較する手段が、前記報知の内容が真実か否かを検知するために、前記報知を行なった投票参加者の投票書類データと、前記入手した暗号化投票書類データ又は暗号化特徴データのうち前記報知した投票参加者のものに該当するデータとを比較する請求項１乃至請求項６のうちのいずれか一項記載の電子投票方式。

【請求項８】　前記１又は複数の情報処理装置において、前記第２の送り手段が、前記投票書類データ又はその特徴データを暗号化して前記調達機関に送るようにする請求項１乃至請求項７のうちのいずれか一項記載の電子投票方式。

【請求項９】　前記第三者機関において、前記公開するための手段が、コンピュータネットワーク上に前記暗号化投票書類データ又は前記暗号化特徴データの各々を公開する請求項１乃至請求項８のうちのいずれか一項記載

の電子投票方式。

【請求項１０】　前記調達機関において、前記公開するための手段が、コンピュータネットワーク上に前記開票結果データを公開する請求項１乃至請求項９のうちのいずれか一項記載の電子投票方式。

【請求項１１】　前記暗号化投票書類データ又は前記暗号化特徴データは、前記第三者機関の公開鍵で暗号化されており、前記第三者機関が、前記開票のときに前記第三者機関の秘密鍵を発行する請求項１乃至請求項１０のうちのいずれか一項記載の電子投票方式。

【請求項１２】　前記１又は複数の情報処理装置において、

前記第１の送り手段が、前記投票書類データ又はその特徴データを自分の秘密鍵又は共通鍵で暗号化して前記第三者機関に送り、

前記第２の送り手段が、前記秘密鍵又は共通鍵で暗号化された投票書類データ又はその特徴データを前記第三者機関の公開鍵で更に暗号化して前記調達機関に送り、

前記調達機関において、

前記開票のときに前記第三者機関の秘密鍵を受けて、その秘密鍵で、前記公開鍵で更に暗号化された前記暗号化投票書類データ又は前記暗号化特徴データの各々を復号化する手段と、

その復号化した前記暗号化投票書類データ又は前記暗号化特徴データの各々を、それらに対応する前記１又は複数の情報処理装置の公開鍵又は共通鍵で復号化する手段とが更に備えられる請求項１乃至請求項１１のうちのいずれか一項記載の電子投票方式。

【請求項１３】　前記１又は複数の情報処理装置と、前記第三者機関と、前記調達機関とがコンピュータネットワークを介して通信可能に接続されており、

前記１又は複数の情報処理装置において、

前記第１の送り手段が、前記投票書類データ又はその特徴データを暗号化してそれを前記コンピュータネットワークを介して前記第三者機関に送信し、

前記第２の送り手段が、前記投票書類データ、その特徴データ、前記暗号化投票書類データ、又は前記暗号化特徴データを暗号化してそれを前記コンピュータネットワークを介して前記調達機関に送信する請求項１乃至請求項１２のうちのいずれか一項記載の電子投票方式。

【請求項１４】　前記開票結果データには、前記開票の際に選出された投票書類データが含まれており、

前記１又は複数の情報処理装置において、前記比較する手段が、前記選出された投票書類データと、前記入手した暗号化投票書類データ又は暗号化特徴データのうち前記選出された投票書類データに対応するデータとを比較する請求項１乃至請求項１３のうちのいずれか一項記載の電子投票方式。

【請求項１５】　前記投票書類データは、入札のときの提出書類の内容を示すデータである請求項１乃至請求項

１４のうちいのいずれか一項記載の電子投票方式。

【請求項１６】　投票書類の内容を記録した投票書類データが暗号化されたものの各々を公開するためのステップと、

前記投票書類データが調達される機関において調達された投票書類データの各々に基づく開票の結果を示すデータを公開するためのステップと、

不正の有無を検知するために、前記公開された暗号化投票書類データと前記公開された開票結果データとを比較するステップとを有する電子投票方法。

【請求項１７】　前記暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成するステップを更に有し、

前記公開するためのステップが、前記生成した証明書の各々を、それらに対応する前記暗号化投票書類データに添付して公開するようにし、

前記比較するステップが、不正の有無を検知するために、前記公開された前記暗号化投票書類データに添付された前記証明書に付けられた日時と、前記開票の日時とを更に比較する請求項１６記載の電子投票方法。

【請求項１８】　投票書類の内容を記録した投票書類データを生成する手段と、

前記投票書類データを暗号化する手段と、

複数の投票参加者の暗号化された投票書類データの各々が公開されたものから暗号化投票書類データを入手するための第１の入手手段と、

投票書類データの各々が調達されたことに基づく開票の結果を示す、公開されたデータを入手するための第２の入手手段と、

不正の有無を検知するために、前記入手した開票結果データと前記暗号化投票書類データとを比較する手段とを備える情報処理装置。

【請求項１９】　第１の入手手段が、投票書類データの存在を証明する証明書が添付された、暗号化書類データを入手し、

前記比較する手段が、不正の有無を検知するために、前記開票の日時と、前記入手した証明書に付けられた日時とを更に比較する請求項１８記載の情報処理装置。

【請求項２０】　前記投票書類データの特徴データを生成する手段を更に備え、

前記暗号化する手段が、前記特徴データを暗号化し、

前記第１の入手手段が、複数の投票参加者の暗号化された特徴データの各々が公開されたものから暗号化特徴データを入手するための、

前記比較する手段が、不正の有無を検知するために、前記開票結果データの特徴データを生成し、その開票結果データの特徴データと、前記入手した暗号化特徴データとを比較する請求項１８記載の情報処理装置。

【請求項２１】　前記証明書には、前記暗号化特徴データの別特徴データが生成された日時と、その日時に生成

した別特徴データを前記暗号化特徴データを用いて生成するための方法とが記録されており、

前記比較する手段が、不正の有無を検知するために、前記存在した日時以後に任意の時に生成された別特徴データが公開されたものから、前記比較の対象の特徴データに対応する証明書に記録された生成日時のときの別特徴データを入手し、且つ、前記比較対象の特徴データとそれの証明書に記録された前記生成方法とに基づいて前記比較対象の特徴データの別特徴データを生成し、その生成した別特徴データと前記入手した別特徴データとを比較する請求項１９又は２０記載の情報処理装置。

【請求項２２】　前記開票の後に、前記投票の参加者から投票書類データの各々が調達された機関において不正があった旨が報知されたときは、

前記第１又は第２の入手手段が、前記報知を行なった投票参加者が保持する投票書類データを入手するようにし、

前記比較する手段が、前記報知の内容が真実か否かを検知するために、前記報知を行なった投票参加者の投票書類データと、前記入手した暗号化投票書類データ又は暗号化特徴データのうち前記報知した投票参加者のものに該当するデータとを比較する請求項１８乃至請求項２１のうちのいずれか一項記載の情報処理装置。

【請求項２３】　信頼される第三者機関と、投票書類の内容を記録した投票書類データを生成する１又は複数の情報処理装置と、前記投票書類データが調達される機関とが備えられるシステム上で、前記情報処理装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体において、

投票書類の内容を記録した投票書類データを生成する手段と、

前記投票書類データを暗号化する手段と、

複数の投票参加者の暗号化された投票書類データの各々が公開されたものから暗号化投票書類データを入手するための第１の入手手段と、

投票書類データが調達されたことに基づく開票の結果を示す、公開されたデータを入手するための第２の入手手段と、

不正の有無を検知するために、前記公開された開票結果データと前記公開された暗号化投票書類データとを比較する手段とを前記コンピュータに実行させるためのプログラムコードを含んだコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の技術分野】本発明は、コンピュータを利用した電子投票の方式に関する。

【０００２】

【従来の技術】コンピュータを利用した電子投票の代表的なものとして、電子入札が知られているが、電子入札

の方式としては、ＴＴＰ（Trusted Third Party、信頼される第三者機関（第三者認証機関））を用いた時間鍵方式が知られている。この方式では、ＴＴＰ、入札参加者、及び調達機関との間で、一般に、図１、２に示すような動作が行なわれている。

【０００３】まず、図１に示すように、ＴＴＰ５が、公開鍵と秘密鍵のペアを作成して（ステップＳ１）、公開鍵のみを調達機関３に送信する（Ｓ２）。その後、調達機関３は、入札参加者１ａ、１ｂ、１ｃから入札参加申請を受けたら（Ｓ３、４、５）、それに対して、ＴＴＰ５から受けた公開鍵をその入札参加者１ａ、１ｂ、１ｃに配布する（Ｓ６、７、８）。

【０００４】各入札参加者１ａ、１ｂ、１ｃは、調達機関３から公開鍵を受取った後、図２に示すように、その公開鍵を使用して入札のための提出書類（以下、入札文書）を暗号化し（ステップＳ９、１０、１１）、それを調達機関３に送信することで入札する（Ｓ１２、１３、１４）。ＴＴＰ５は、開札時刻になったときに、秘密鍵を調達機関３に送信する（Ｓ１５）。調達機関３は、ＴＴＰ５からの秘密鍵を使用して公開鍵で暗号化されている入札文書を復号化し、開札を行なう（Ｓ１６）。

【０００５】

【発明が解決しようとする課題】入札では、不正の防止が何よりも望まれることである。しかし、上述した電子入札は、以下のような不正が行われても、これを電子的に発見し防止することができない。

【０００６】（１）調達機関３が、受け付けた入札文書を開札後に改竄することとにより、調達機関３が、ある入札参加者１ａと不正に契約を結んで、その参加者１ａが落札できるよう入札文書に改竄することが可能になってしまう。

【０００７】（２）調達機関３が、提出期限を過ぎているにも拘わらず入札文書を受け付けることとにより、ある入札参加者１ａが、何らかの方法で他の入札参加者１ｂ、１ｃの動向を探り、他の入札参加者１ｂ、１ｃが入札文書を調達機関３に提出した後に、それに応じて、自分に都合の良い文書を作成して入札することが可能になってしまう。

【０００８】（３）入札参加者１ａ、１ｂ、１ｃが、入札又は開札後に、自分の手元にある入札文書の内容を不正に改竄することとにより、入札参加者１ａ、１ｂ、１ｃは、落札できなかった場合に、「現在、調達機関３に存在している入札文書は、調達機関３で不正に改竄されたものであり、自分が入札したものとは異なる」と主張することが可能になってしまう。

【０００９】従って、本発明の目的は、上記不正を確実に検証できる信頼性の高い電子入札を提供することにある。

【００１０】

【課題を解決するための手段】本発明の第１の側面に従

う電子投票方式では、投票書類の内容を記録した投票書類データを生成する１又は複数の情報処理装置と、信頼される第三者機関と、前記投票書類データが調達される機関とを備え、第三者機関が、暗号化された投票書類データを公開するための手段を備え、調達機関が、調達された投票書類データに基づく投票結果を示すデータを公開するための手段を備え、１又は複数の情報処理装置が、投票書類データを暗号化してそれを第三者機関に送るための手段と、投票書類データを調達機関に送るための手段と、公開された暗号化投票書類データを入手するための手段と、公開された投票結果データを入手するための手段と、不正の有無を検知するために、暗号化投票書類データと投票結果データとを比較する手段とを備える。

【００１１】例えば、１又は複数の情報処理装置は、投票書類データを信頼される第三者機関に送るときは、第三者機関の公開鍵や自分の共通鍵又は秘密鍵で暗号化した投票書類データを、フロッピーディスクやＭＯ等の記録媒体に記録してその記録媒体を郵送などで送るようにしたり、コンピュータネットワーク（典型的にはインターネット）を介して送信したりする。また、１又は複数の情報処理装置は、投票書類データを調達機関に送るときは、投票書類データを、フロッピーディスク等の記録媒体に記録してその記録媒体を郵送などで送るようにしたり、第三者機関の公開鍵で暗号化、或いは自分の共通鍵又は秘密鍵で暗号化（更に第三者機関の公開鍵で暗号化してもよい）してからそれをコンピュータネットワークを介して送信したりする。第三者機関は、送られて来た各記録媒体に記録された、又はコンピュータネットワークを介して送られて来た暗号化投票書類データを、コンピュータネットワーク上に、特定の雑誌上に、又はＣＤ－ＲＯＭやＭＯ等の記録媒体に記録して各入札参加社宛に郵送等で送って直接的に、のいずれかの方法で公開するようにする。調達機関は、郵送等で送られて来た各記録媒体に記録された、又はコンピュータネットワークを介して送られて来た投票書類データの各々に基づく開票の結果を示すデータ（例えば、調達機関で調達された投票書類データの全て、又は開票において選出された投票書類データのみ）を、コンピュータネットワーク上に、特定の雑誌上に、又はＣＤ－ＲＯＭやＭＯ等の記録媒体に記録して各入札参加社宛に郵送等で送って直接的に、のいずれかの方法で公開するようにする。１又は複数の情報処理装置は、第三者機関、及び調達機関によって行なわれる上記公開により、開票結果データと、投票参加者の暗号化投票書類データとを入手し、不正の有無を検知するために、開票結果データと暗号化投票書類データとを比較する。比較するときは、例えば、各投票参加者の共通鍵又は公開鍵で、暗号化投票書類データの各々を復号化してから、上記比較をする。この結果、実質的に一致しないデータが含まれていれば、投票書類データが不正に改竄されたということを検知することができる。

【００１２】好適な実施形態では、第三者機関において、暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成する手段が更に備えられ、公開するための手段が、生成した証明書の各々を、それらに対応する暗号化投票書類データに添付して公開するようにする。この場合、１又は複数の情報処理装置において、第１の入手手段が、公開された暗号化投票書類データと共に証明書を入手し、比較する手段が、不正の有無を検知するために、開票の日時と、入手した証明書に付けられた日時とを更に比較する。これにより、証明書に付けられた日時が開票日時よりも遅い日時であるものが含まれていれば、開票日時が過ぎたにも拘わらずに不正に受け付けられた投票書類データがあることを検知することができる。

【００１３】好適な実施形態では、１又は複数の情報処理装置において、投票書類データの特徴データを生成する手段が更に備えられ、第１の送り手段が、特徴データを暗号化したものを第三者機関へ送るようにする。第三者機関において、公開するための手段が、暗号化特徴データの各々を公開するようにする。この場合、１又は複数の情報処理装置において、第１の入手手段が、公開された暗号化特徴データを入手し、比較する手段が、不正の有無を検知するために、開票結果データの特徴データを生成し、その開票結果データの特徴データと、入手した暗号化特徴データとを比較する。

【００１４】好適な実施形態では、第三者機関において、上記証明書に付けられた日時以後、任意の時に暗号化特徴データの別特徴データを生成する手段と、その任意の時に生成した別特徴データを公開するための手段が更に備えられ、証明書を生成する手段が、暗号化特徴データの各々に対し、暗号化特徴データの別特徴データを生成した日時と、その日時に生成した別特徴データをその暗号化特徴データを用いて生成するための方法とを記録した証明書（例えばＳＨＶ証明書）を生成する。この場合、１又は複数の情報処理装置において、比較する手段が、不正の有無を検知するために、公開された別特徴データから、比較の対象の特徴データ1対応する証明書に記録された生成日時のときの別特徴データを入手し、且つ、比較対象の特徴データとそれの証明書に記録された生成方法とに基づいて比較対象の特徴データの別特徴データを生成し、その生成した別特徴データと上記入手した別特徴データとを比較する。なお、別特徴データを生成する手段は、定期的に（例えば１秒毎）別特徴データを生成しても良い。

【００１５】好適な実施形態では、特徴データ又は別特徴データは、ハッシュ値である。

【００１６】好適な実施形態では、１又は複数の情報処理装置において、第２の送り手段が、入手した証明書の

うち、生成した投票書類データに対応する証明書をその投票書類データに添付して、それを調達機関に送るようにする。

【0017】好適な実施形態では、開票の後に、投票参加者から不正があった旨（例えば調達機関で自分の投票書類データが改竄された旨）が報知（提起）されたときは、1又は複数の情報処理装置において、第1又は第2の入手手段が、上記報知（提起）を行なった投票参加者が保持する投票書類データを入手（例えばコンピュータネットワークを介してその投票書類データを受信）するようにし、比較する手段が、報知の内容が真実か否かを検知するために、上記報知を行なった投票参加者の投票書類データと、入手した暗号化投票書類データ又は暗号化特徴データのうち報知した投票参加者のものに該当するデータとを比較する。

【0018】好適な実施形態では、1又は複数の情報処理装置において、第2の送り手段が、投票書類データ又はそれの特徴データを暗号化して調達機関に送るようにする。

【0019】好適な実施形態では、第三者機関において、公開するための手段が、コンピュータネットワーク上に暗号化投票書類データ又は暗号化特徴データの各々を公開する。また、調達機関において、公開するための手段が、コンピュータネットワーク上に開票結果データを公開する。

【0020】好適な実施形態では、暗号化投票書類データ又は暗号化特徴データは、第三者機関の公開鍵で暗号化されており、第三者機関が、開票のときに第三者機関の秘密鍵を（調達機関、或いは1又は複数の情報処理装置に）発行する。

【0021】好適な実施形態では、1又は複数の情報処理装置において、第1の送り手段が、投票書類データ又はそれの特徴データを自分の（投票書類データを送るための情報処理装置の）秘密鍵又は共通鍵で暗号化して第三者機関に送り、第2の送り手段が、その自分の秘密鍵又は共通鍵で暗号化された投票書類データ又はそれの特徴データを第三者機関の公開鍵で更に暗号化して調達機関に送る。この場合、調達機関において、開票のとき（より好適には開票日時）に第三者機関の秘密鍵を受けて、その秘密鍵で、第三者機関の公開鍵で更に暗号化された暗号化投票書類データ又は暗号化特徴データの各々を復号化する手段と、その復号化した暗号化投票書類データ又は暗号化特徴データの各々を、それらに対応する1又は複数の情報処理装置の公開鍵又は共通鍵で復号化する手段とが更に備えられる。

【0022】好適な実施形態では、1又は複数の情報処理装置と、第三者機関と、調達機関とがコンピュータネットワークを介して通信可能に接続されており、1又は複数の情報処理装置において、第1の送り手段が、投票書類データ又はそれの特徴データを暗号化してそれをコンピュータネットワークを介して第三者機関に送信し、第2の送り手段が、投票書類データ、それの特徴データ、暗号化投票書類データ、又は暗号化特徴データを暗号化してそれをコンピュータネットワークを介して調達機関に送信する。

【0023】好適な実施形態では、開票結果データには、開票の際に選出された投票書類データが含まれており、1又は複数の情報処理装置において、比較する手段が、選出された投票書類データと、入手した暗号化投票書類データ又は暗号化特徴データのうち上記選出された投票書類データに対応するデータとを比較する。

【0024】好適な実施形態では、投票書類データは、入れのときの提出書類の内容を示すデータである。

【0025】本発明に従う電子投票方法では、投票書類の内容を記録した投票書類データが暗号化されたものの各々を公開するためのステップと、投票書類データが調達される機関において調達された投票書類データの各々に基づく開票の結果を示すデータを公開するためのステップと、不正の有無を検知するために、公開された暗号化投票書類データと公開された開票結果データとを比較するステップとを有する。

【0026】好適な実施方法では、暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成するステップを更に有し、公開するためのステップが、生成した証明書の各々を、それらに対応する暗号化投票書類データに添付して公開するようにし、比較するステップが、不正の有無を検知するために、公開された暗号化投票書類データに添付された証明書に付けられた日時と、開票の日時とを比較する。

【0027】

【発明の実施の形態】図3は、本発明の一実施形態に係る電子入れ方式における全体的なシステム構成を示す。

【0028】各入れ参加者が利用する端末装置11a、11b、11c、…、TTP（Trusted Third Party、第三者認証機関）15、及び調達機関13が、通信ネットワーク（典型的にはインターネット）27によって通信可能に接続されている。

【0029】端末装置11a、11b、11c、…は、典型的には、殆どどの会社にも設置されている汎用コンピュータ（例えばパーソナルコンピュータ）であって、後述する種々の動作、例えば、入れにおける提出書類の内容を示す文書データ（本明細書で言う「文書」は、文字データに限定されず、画像データ等も含む）のハッシュ値を生成したり（以下、ハッシュ文書という）、そのハッシュ文書をその入れ参加者の秘密鍵で暗号化（以下、暗号化ハッシュ文書という）してそれをTTP15に送信したりする等の機能を備えている。以下の説明では、分かり易くするため、入れ参加者を、「A社」、「B社」、「C社」の各会社とし、端末装置11a、1

１ｂ、１１ｃを、それぞれA社、B社、C社の「入札端末」と呼ぶことにする。

【００３０】ＴＴＰ１５には、コンピュータネットワーク（例えばＬＡＮ）２５が設けられており、そのネットワーク２５には、入札支援サーバ１９、タイムスタンプサーバ２１、及びデータベース２３が接続されている。

【００３１】入札支援サーバ１９は、主に、調達機関１３での不正の可能性を無くすことに貢献している。即ち、入札支援サーバ１９は、公開鍵・秘密鍵を作成して、はじめに、各入札参加社の上記暗号化ハッシュ文書を暗号化させるための公開鍵を調達機関１３に送信し、開札時刻になったときに、公開鍵で暗号化された暗号化ハッシュ文書を復号化するための秘密鍵を調達機関１３に送信する。また、入札支援サーバ１９は、各入札端末１１ａ、１１ｂ、１１ｃからの暗号化ハッシュ文書を、後述するＳＨＶ証明書を添付して、インターネット２７上に公開する。

【００３２】タイムスタンプサーバ２１は、主に、各入札端末提出１１ａ、１１ｂ、１１ｃからの入札文書の存在とその時刻、及び入札文書の内容が改竄されていないことを証明することを行なう。ここで、タイムスタンプサーバ２１には、米国のSurety社が開発したDigital Notary Service（電子文書証明サービス、以下、ＤＮＳ）における特表平１０－５０８１２１号公報記載の技術が導入されている。即ち、タイムスタンプサーバ２１は、各入札端末１１ａ、１１ｂ、１１ｃからの暗号化ハッシュ文書を受信したら、それのＳＨＶ（Super Hash Value、スーパーハッシュ値）を生成し、更に、その暗号化ハッシュ文書に対するＳＨＶ証明書を作成する。尚、ＳＨＶとは、ＤＮＳでのタイムスタンプ技術において生成されるハッシュ値のことである。

【００３３】図４に、ＳＨＶ証明書の構成の一例を示す。

【００３４】タイムスタンプサーバ２１は、例えば、暗号化ハッシュ文書のＳＨＶを算出するためのＳＨＶ算出情報３１、そのＳＨＶを算出した日付・時刻（つまりそのＳＨＶの存在を証明する日付・時刻）３３、及びユーザＩＤ３５などをＳＨＶ証明書３７に掲載する。ＳＨＶ算出情報３１として、ＳＨＶ算出の因子となる複数のハッシュ値や、その各ハッシュ値を用いるＳＨＶ算出の計算経路（計算手順）が示される。このＳＨＶ証明書に掲載されるＳＨＶ算出情報３１、及び日付・時刻３３は、例えば、暗号化ハッシュ文書が受信されて最初にＳＨＶが算出されてから１秒後の、ＳＨＶ算出情報、及び日付・時刻である。

【００３５】ＳＨＶ証明書３７に基づいたＳＨＶの算出方法に関しては、上記特表平１０－５０８１２１号公報に記載のものを利用する。図５に、概略的にその一例を示す。

【００３６】図４に示したＳＨＶ証明書３７が添付されている暗号化ハッシュ文書２００のＳＨＶを、その証明書３７に基づいて算出するときは、例えば次のようにして行なう。

【００３７】まず、証明書３７のＳＨＶ算出情報３１に指定された第１の因子ハッシュ値（例えば「abcdef…」）２０３を抽出し、そのハッシュ値２０３と、暗号化ハッシュ文書のハッシュ値（例えば「ABCDE…」）２０１とを連結してハッシュをとり、連結したもののハッシュ値（例えば「AbCdEf…」）２０５を生成する。

【００３８】次に、ＳＨＶ算出情報３１に指定された第２の因子ハッシュ値（例えば「aZbYcX…」）２０７と、上記生成したハッシュ値２０５とを連結してハッシュをとり、連結したもののハッシュ値（例えば「abbdcf…」）２０９を生成する。このようなハッシュ値の連結及び生成は、ＳＨＶ算出情報３１に指定された計算経路に従って行なっていく。

【００３９】そして、最後は、最終的に生成したハッシュ値（例えばハッシュ値２０９）と、証明書３７に記載されている日付・時刻（以下、当該時刻という）の１秒前のＳＨＶ２１１とを連結してハッシュをとり、当該時刻におけるＳＨＶ２１３を生成する。なお、当該時刻の１秒前のＳＨＶ２１１とは、後の説明でわかるとおり、タイムスタンプサーバ２１が暗号化ハッシュ文書を受けてから入札審査が終了するまでの間に毎秒（つまり１秒毎に）作成するＳＨＶにおいて、当該時刻の１秒前に該当するものである。

【００４０】再び図３を参照して、タイムスタンプサーバ２１は、入札端末１１ａ、１１ｂ、１１ｃからの各暗号化ハッシュ文書に対して、図４に示したようなＳＨＶ証明書を作成したら、それを入札支援サーバ１９に渡す。これにより、この後、入札支援サーバ１９は、上述したように、タイムスタンプサーバ２１から渡された各ＳＨＶ証明書を、入札端末１１ａ、１１ｂ、１１ｃからの暗号化ハッシュ文書にそれぞれ添付し、暗号化ハッシュ文書とＳＨＶ証明書のペアをインターネット２７上に公開する。

【００４１】また、タイムスタンプサーバ２１は、各暗号化ハッシュ文書に対し、暗号化ハッシュ文書を受けてから入札審査が終了するまでの間、暗号化ハッシュ文書のＳＨＶの生成を毎秒（つまり１秒毎に）行い、それをデータベース２３に保存する。そして、タイムスタンプサーバ２１は、不正に改竄されたか否かの検証が必要とされる暗号化ハッシュ文書の１秒毎のＳＨＶを、インターネット２７上に公開する。

【００４２】ＴＴＰ１５は、入力支援サーバ１９とタイムスタンプサーバ２１の上述した各々の機能によって、この電子入札において不正が行われてもそれを確実に検証できるようにする。例えば、調達機関１３が提出期限を過ぎているにも拘わらず不正に入札文書を受けたとしても、各入札参加社が、インターネット２７上に公開さ

れている各入札文書（暗号化ハッシュ文書）のＳＨＶ証明書上の、文書存在を証明する日付・時刻を確認することで、その不正を検証できる。

【００４３】調達機関１３は、調達サーバ１７を備えている。調達サーバ１７は、ＴＴＰ１５からの公開鍵を受けてそれを各入札端末１１ａ、１１ｂ、１１ｃに配布し、その公開鍵によって暗号化された暗号化ハッシュ文書を各入札端末１１ａ、１１ｂ、１１ｃから受ける。調達サーバ１７は、開札時刻になったら、ＴＴＰ１５から秘密鍵を受け、その秘密鍵で、それら暗号化された暗号化ハッシュ文書を復号化する。そして、調達サーバ１７は、入札参加社の秘密鍵で暗号化された各暗号化ハッシュ文書を、その入札参加社の公開鍵で復号化して、各入札に対する審査を行なえるようにする。また、その審査が終了して落札社が決定したときは、調達サーバ１７は、入札の審査結果（例えば、決定された落札社の会社名、落札社の入札文書等）を、インターネット２７上に公開する。

【００４４】以下、図６～図１０を参照して、上述したシステム様成において行なわれる電子入札の手順を具体的に説明する。

【００４５】まず、図６に示すようにＴＴＰ１５の入札支援サーバ１９が、公開鍵・秘密鍵を作成し（ステップＳ２１）、そのうち公開鍵のみを調達機関１３に送付する（Ｓ２２）。調達機関１３の調達サーバ１７は、ＴＴＰ１５からの公開鍵を、各入札端末１１ａ、１１ｂ、１１ｃに配布する（Ｓ２４、２５、２６）。

【００４６】その後、各入札端末１１ａ、１１ｂ、１１ｃは、図７に示すように、入札する文書のハッシュをとってそれのハッシュ値を生成し（ステップＳ２７、２８、２９）、それを自社の秘密鍵で暗号化する（Ｓ３０、３１、３２）。そして、各入札端末１１ａ、１１ｂ、１１ｃは、自社の秘密鍵により暗号化した暗号化ハッシュ文書を、インターネット２７を介してＴＴＰ１５に送信する（Ｓ３３、Ｓ３４、Ｓ３５）。

【００４７】ＴＴＰ１５では、図８に示すように、タイムスタンプサーバ２１が、各入札端末１１ａ、１１ｂ、１１ｃからの暗号化ハッシュ文書について、それぞれに図４に示したようなＳＨＶ証明書を作成し（ステップＳ３６）、それを入札支援サーバ１９に渡す（Ｓ３７）。入札支援サーバ１９は、各暗号化ハッシュ文書に、タイムスタンプサーバ２１から渡されたＳＨＶ証明書をそれぞれ添付し、暗号化ハッシュ文書とＳＨＶ証明書のペアをインターネット２７上に公開する（Ｓ３８）。この公開の方法としては、例えばこの図に示すように、入札支援サーバ１９は、ＴＴＰ１５のホームページ１０１上に、各参加社の暗号化ハッシュ文書とＳＨＶ証明書とのペア１０３ａ、１０３ｂ、１０３ｃを掲載する。各参加社は入札端末１１ａ、１１ｂ、１１ｃを利用して、ＴＴＰ１５によって公開された全ての参加社のデータ１０３ａ、１０３ｂ、１０３ｃをダウンロードする（Ｓ３９、４０、４１）。

【００４８】一方で、ＴＴＰ１５のタイムスタンプサーバ２１は、各入札端末１１ａ、１１ｂ、１１ｃからの暗号化ハッシュ文書について、例えば上記特表平１０－５０８１２１号公報に記載の方法を利用して、毎秒（つまり１秒毎に）ＳＨＶを算出する（Ｓ４２）。タイムスタンプサーバ２１は、その方法により算出した各暗号化ハッシュ文書の毎秒のＳＨＶを、データベース２３に保存すると共に（Ｓ４３）、インターネット２７上に公開する（Ｓ４４）。この公開の方法としては、例えばこの図に示すように、ＴＴＰ１５のホームページ１１０を用意し、そのホームページ１１０上に、所望のＳＨＶ証明書のユーザＩＤを入力させて所望の参加社の公開ＳＨＶデータ１１１を表示する。公開ＳＨＶデータ１１１は、ＴＴＰ１５が入札文書を受けてから入札審査が終了するまでの毎秒の暗号化ハッシュ文書のＳＨＶである。尚、この公開ＳＨＶデータ１１１は、ＣＤ－ＲＯＭ等の記録媒体に記録させて、その記録媒体を全参加社に配布する等するようにしても良い。

【００４９】各入札端末１１ａ、１１ｂ、１１ｃは、調達機関１３に入札するときは、図９に示すように、暗号化ハッシュ文書に電子署名（ステップＳ４５、４６、４７）、それを調達機関から配布されたＴＴＰ１５発行の公開鍵を使用して暗号化する（Ｓ４８、４９、５０）。そして、各入札端末１１ａ、１１ｂ、１１ｃは、その暗号化ハッシュ文書を調達機関１３に送信することで入札を行なう（Ｓ５１、５２、５３）。なお、この図において、各入札端末１１ａ、１１ｂ、１１ｃは、自分の暗号化ハッシュ文書に対応するＳＨＶ証明書をＴＴＰ１５から入手し、そのＳＨＶ証明書と共に、自分の暗号化ハッシュ文書を調達機関１３に送信することもできる。これにより、調達機関１３は、各入札端末１１ａ、１１ｂ、１１ｃからＳＨＶ証明書付きの暗号化ハッシュ文書を受けることになるので、それらＳＨＶ証明書に基づいて上記方法で各暗号化ハッシュ文書のＳＨＶを求め、求められたＳＨＶと、公開ＳＨＶデータ１１１からＳＨＶ証明書に記録された日付・時刻のＳＨＶを取得したものとを比較することで、各入札端末１１ａ、１１ｂ、１１ｃから送られて来た入札文書が不当に改竄されていないかどうかを確認することができる。また、調達機関１３は、後述する入札審査結果の公開のときに、ＳＨＶ証明書も併せて公開することができるので、各参加社に対する透明性をより高めることができる。

【００５０】開札時刻になったら、図１０に示すように、ＴＴＰ１５の入札支援サーバ１９が、秘密鍵を調達機関１３に送付する（ステップＳ５４）。調達機関１３の調達サーバ１７は、ＴＴＰ１５からの秘密鍵を使用して、ＴＴＰ１５の公開鍵によって暗号化されている各入札端末１１ａ、１１ｂ、１１ｃからの暗号化ハッシュ文

書を復号化する（Ｓ５５）。それにより、復号化された各暗号化ハッシュ文書は、各参加者の秘密鍵によって暗号化されているハッシュ文書となる。そこで、調達サーバ１７は、それらの暗号化ハッシュ文書を、それの入札参加社の公開鍵で復号化して（Ｓ５６）、各入札に対する審査を可能な状態にする。調達サーバ１７は、その審査が終了して落札する社が決定したときは、その審査の結果を各入札参加社に対して公開する（Ｓ５７）。この公開の方法としては、例えばこの図に示すように、調達サーバ１７は、調達機関１３のホームページ１０５上に、入札審査の結果、例えば落札社の入札文書（納品物に関する提案書、技術仕様書、受注金額など）１０７を掲載する。勿論、調達サーバ１７は、入札審査の結果として、全ての入札参加社の入札文書をホームページ１０５上に掲載するようにしてもよい。この場合は、後述する不正の検証において、各入札参加社は、入札端末１１ａ、１１ｂ、１１ｃを利用して、その入札審査結果をダウンロードし、その審査結果として（つまり開札後）の全ての入札参加社の入札文書と、既に保持している開札前の全参加社の入札文書（暗号化ハッシュ文書）とを比較して、不正の有無を検証することができる。

【００５１】各入札参加社は、入札端末１１ａ、１１ｂ、１１ｃを利用して、この電子入札において、不正が行なわれたか否かを検証できるように、落札社の入札文書１０７をダウンロードする（Ｓ５８、５９、６０）。

【００５２】この実施形態における電子入札では、従来検証できなかった以下の不正を検証することができる。その不正の検証について説明する。

【００５３】（１）調達機関３が、受け付けた入札文書を開札後に改竄すること。

【００５４】これについては、各入札参加社が、入札端末１１ａ、１１ｂ、１１ｃを利用して検証できる。それについて、図１１を参照して説明する。

【００５５】入札端末１１ａ、１１ｂ、１１ｃは、図１０のステップＳ５８、５９、６０で、落札社の入札文書１０７をダウンロードした。そこで、入札端末１１ａ、１１ｂ、１１ｃは、その落札社入札文書１０７のハッシュをとって、開札後の落札社入札文書のハッシュ値を生成する（ステップＳ６１）。

【００５８】また、入札端末１１ａ、１１ｂ、１１ｃは、図８のステップＳ３９、４０、４１で、全参加社の暗号化ハッシュ文書及びそのＳＨＶ証明書のペア１０３ａ、１０３ｂ、１０３ｃをダウンロードした。各暗号化ハッシュ文書は、その参加社の秘密鍵で暗号化された文書である。そこで、入札端末１１ａ、１１ｂ、１１ｃは、ダウンロードした暗号化ハッシュ文書のうち落札社の暗号化ハッシュ文書を、その落札者の公開鍵で復号化して、開札前の落札社入札文書のハッシュ値を得る。

【００５７】入札端末１１ａ、１１ｂ、１１ｃは、落札社入札文書の、開札後のハッシュ値と開札前のハッシュ値とを比較し、それらが一致していなければ、落札社の入札文書は開札後に改竄されたと判断する（Ｓ６３）。

【００５８】このようにして、各入札参加社は、この電子入札における不正を検証することができる。

【００５９】（２）調達機関３が、提出期限が過ぎているにも拘わらず入札文書を受け付けること。

【００６０】これについては、各入札参加社が、入札端末１１ａ、１１ｂ、１１ｃを利用して検証できる。入札端末１１ａ、１１ｂ、１１ｃは、落札社のＳＨＶ証明書に記録されている日付・時刻の正当性を証明し、その時刻が開札時刻の前・後のどちらであるかを参加社に確認してもらうことでこの不正を検証できるようにする。これについて、図１２を参照して説明する。

【００６１】入札端末１１ａ、１１ｂ、１１ｃは、図１１に示したステップＳ６３の動作を終えた後に、この不正の検証を行なうことができる。入札端末１１ａ、１１ｂ、１１ｃは、図１１のステップＳ６３の後、公開ＳＨＶデータ１１１が掲載されているホームページ１１０（図８参照）にアクセスし、落札社のＳＨＶ証明書に記録されているユーザＩＤをキーに、落札社の公開ＳＨＶデータ１１１を取得し、そのデータから落札社のＳＨＶ証明書の日付・時刻の正当性を証明するために必要なＳＨＶを得る（ステップＳ６４）。その必要なＳＨＶは、当該時刻（つまり証明書の日付・時刻）でのＳＨＶとその時刻の１秒前のＳＨＶである。入札端末１１ａ、１１ｂ、１１ｃは、落札社の暗号化ハッシュ文書、それに添付されているＳＨＶ証明書中のＳＨＶ算出情報（図４参照）、及び当該時刻の１秒前のＳＨＶを用いて、例えば図５を参照して説明した方法により、当該時刻のＳＨＶを算出する（Ｓ６５）。

【００６２】その後、入札端末１１ａ、１１ｂ、１１ｃは、その算出した当該時刻のＳＨＶと、ステップＳ６４で公開データ１１１から取得した当該時刻のＳＨＶとを比較し、それらが一致していれば、落札社のＳＨＶ証明書中の日付・時刻は正当なものであると証明する（Ｓ６６－ａ）。そして、その証明された時刻と開札時刻とを比較し、その証明された時刻が開札時刻の後であれば、落札社の入札文書は提出期限が過ぎているにも拘わらず調達機関１３で不正に受付られたものと判断する（Ｓ６６－ｂ）。

【００６３】（３）ある参加社が、入札又は開札後に、自分の手元にある入札文書の内容を不正に改竄すること。

【００６４】例えば、Ｂ社が、落札社決定後に自分の手元にある入札文書を不正に改竄しその入札文書が本物であると主張しているとする。他の参加社であるＡ社、Ｃ社は、自社の入札端末１１ａ、１１ｃを利用してその主張は正当なものか否かを検証できる。それについて、図１３を参照して説明する。

【００６５】まず、Ｂ社が、自社の入札端末１１ｂを利

用して、本物であると主張しているＢ社主張入札文書３００をインターネット２７上にダウンロードするようにする（ステップＳ６７）。

【００６６】他の参加社であるＡ社、Ｃ社は、自社の入札端末１１ａ、１１ｃを利用して、Ｂ社主張入札文書３００をダウンロードし（Ｓ６８、Ｓ７２）、Ｂ社主張入札文書３００のハッシュ値を生成する（Ｓ６９、Ｓ７３）。その後、以前にダウンロードしたＢ社の暗号化ハッシュ文書をＢ社の公開鍵で復号化して、Ｂ社の当初の入札文書のハッシュ値を得る（Ｓ７０、Ｓ７４）。そして、そのＢ社の当初入札文書のハッシュ値と、ステップＳ６９、７３で生成したＢ社主張入札文書のハッシュ値とを比較し、それらが一致していなければ、Ｂ社の主張は不当であると判断する（Ｓ７１、Ｓ７５）。

【００６７】このように、ある参加社が入札又は開札後に自分の手元にある入札文書の内容を不正に改竄しても、他の参加社がその不正を検証することができる。これにおいて、Ｂ社が上記主張を正当であるとするためには、他の参加社Ａ社、Ｃ社が各々保有するＢ社の暗号化ハッシュ文書の全てをＢ社主張の入札文書に取り替えなければならない。これを行なうのは実質的に不可能なので、上記不当な主張が行なわれることを未然に防ぐことが図れる。

【００６８】上述した実施形態によれば、従来検証することができなかった上記種々の不正を、各参加社が検証できるので、電子入札の信頼性を高めるられると共に、上記種々の不正が行なわれることを未然に防ぐことが図れる。

【００６９】また、上述した実施形態によれば、ＴＴＰ１５が、不正の検証に必要なデータ（各参加者の開札前の入札文書データ（暗号化ハッシュ文書）、ＳＨＶ証明書、公開ＳＨＶデータ１１１）を公開する。このため、極めて信頼性の高いデータが公開されるので入札における透明性が高まり、また、裁判ではそのデータを証拠としても利用できる可能性が高いので、安全性・信頼性の高い電子入札が可能になる。

【００７０】以上、本発明の好適な幾つかの実施形態を説明したが、これらは本発明の説明のための例示であって、本発明の範囲をこれらの実施例にのみ限定する趣旨ではない。本発明は、他の種々の形態でも実施することが可能である。すなわち、本発明を入札に適用としたときの一実施形態の説明からもわかるように、本発明は、電子投票において行なわれ得る実質的に全ての不正を検証できるものである。従って、本発明は、あらゆる投票の態様に適用することが可能であり、選挙のような不正が絶対にあってはならないものにこそ本発明は適用価値がある。仮に、選挙に適用すれば、信頼性・安全性の高い選挙が保証されるだけでなく、選挙権者は通信端末装置さえ持っていればどこからでも投票可能になるので、わざわざ選挙会場まで足を運ぶ必要が無くなり、投票率の向上が期待できる。

【図面の簡単な説明】

【図１】従来の電子入札における動作説明図。

【図２】従来の電子入札における動作説明図。

【図３】本発明の一実施形態に係る電子入札方式における全体的なシステム構成を示すブロック図。

【図４】ＳＨＶ証明書の構成の一例を示す図。

【図５】ＳＨＶ証明書に基づいたＳＨＶの算出方法を説明するための図。

【図６】各入札端末１１ａ、１１ｂ、１１ｃにＴＴＰ１５の公開鍵が配布されるときの動作を示す図。

【図７】各入札端末１１ａ、１１ｂ、１１ｃがＴＴＰ１５に暗号化ハッシュ文書を送信するときの動作を示す図。

【図８】ＴＴＰ１５が各参加社の暗号化ハッシュ文書やそれのＳＨＶを公開するときの動作を示す図。

【図９】各入札端末１１ａ、１１ｂ、１１ｃによって入札が行なわれるときの動作を示す図。

【図１０】入札審査の結果が公開されるときの動作を示す図。

【図１１】各入札端末１１ａ、１１ｂ、１１ｃが、調達機関３が受け付けた入札文書を開札後に改竄することを検証するときの動作を示すフローチャート。

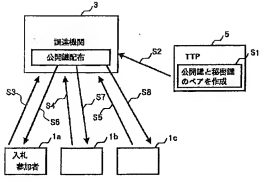
【図１２】各入札端末１１ａ、１１ｂ、１１ｃが、調達機関３が提出期限を過ぎているにも拘わらず入札文書を受け付けることを検証するときの動作を示すフローチャート。

【図１３】ある参加社が入札又は開札後に自分の手元にある入札文書の内容を不正に改竄することを検証するときの動作を示すフローチャート。

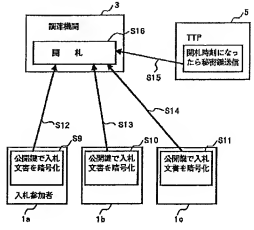
【符号の説明】

１１ａ、１１ｂ、１１ｃ　入札端末
１３　調達機関
１５　ＴＴＰ
１７　調達サーバ
１９　入札支援サーバ
２１　タイムスタンプサーバ
２７　インターネット
３７　ＳＨＶ証明書

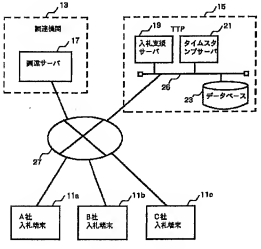
【図１】


3
調達機関
公開鍵配布
5
TTP
公開鍵と秘密鍵のペアを作成
S1
S2
S3
S4
S5
S6
S7
S8
入札参加者
1a
1b
1c

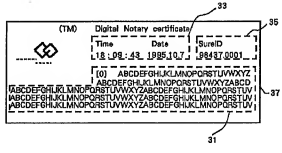
【図２】


3
調達機関
S16
開　札
5
TTP
開札時刻になったら秘密鍵送信
S15
S14
S12
S13
S9
S10
S11
公開鍵で入札文書を暗号化
公開鍵で入札文書を暗号化
公開鍵で入札文書を暗号化
入札参加者
1a
1b
1c

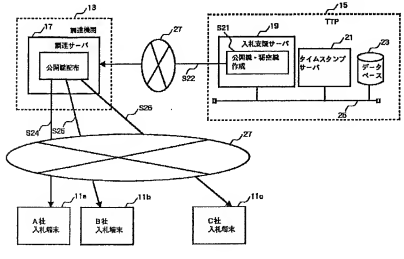
【図３】


13
調達機関
17
調達サーバ
15
TTP
19
入札支援サーバ
21
タイムスタンプサーバ
23
データベース
27
11a
11b
11c
A社入札端末
B社入札端末
C社入札端末

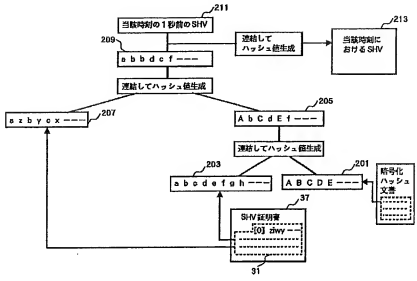
【図４】


33
(TM)
Digital Notary certificate
35
Time
Date
SureID
15:09:49
1995.10.7
9848170501
[0]
ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZABCD
EFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUV
37
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUV
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUV
31

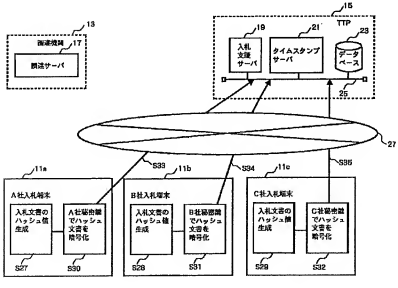
【図６】


13
調達機関
17
調達サーバ
公開鍵配布
27
15
TTP
S21
19
入札支援サーバ
公開鍵・秘密鍵作成
21
タイムスタンプサーバ
23
データベース
S22
25
S26
S24
S25
27
11a
11b
11c
A社入札端末
B社入札端末
C社入札端末

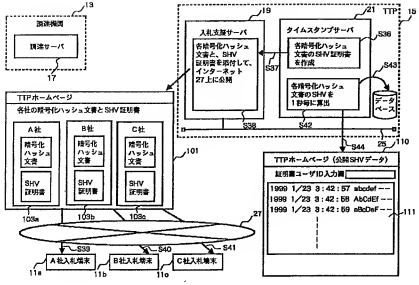
【図５】


211
当該時刻の１秒前のSHV
213
当該時刻における SHV
連結して
ハッシュ値生成
209
a b b d c f ---
連結してハッシュ値生成
205
A b C d E f ---
207
a z b y c x ---
連結してハッシュ値生成
203
a b o d e f g h ---
201
A B C D E ---
暗号化
ハッシュ
文書
37
SHV証明書
101 zwy --
31

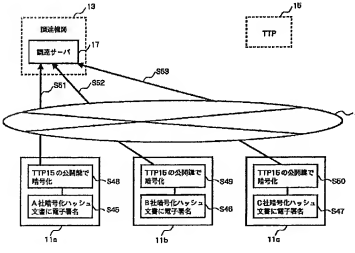
【図７】


15
TTP
13
認証機関
17
認証サーバ
19
入札
公開
サーバ
21
タイムスタンプ
サーバ
23
データ
ベース
25
27
S33
S34
S35
11a
A社入札端末
入札文書の
ハッシュ値
生成
A社秘密鍵
でハッシュ
文書を
暗号化
S27
S30
11b
B社入札端末
入札文書の
ハッシュ値
生成
B社秘密鍵
でハッシュ
文書を
暗号化
S28
S31
11c
C社入札端末
入札文書の
ハッシュ値
生成
C社秘密鍵
でハッシュ
文書を
暗号化
S29
S32

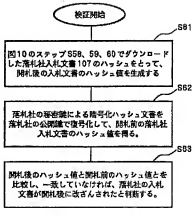
【図８】


13
調達機関
調達サーバ
17
15
TTP
19
入札支援サーバ
各暗号化ハッシュ文書と、SHV証明書を添付して、インターネット27上に公開
21
タイムスタンプサーバ
各暗号化ハッシュ文書のSHV証明書を作成
S36
S37
S43
各暗号化ハッシュ文書のSHVを1秒毎に算出
データベース
S38
S42
TTPホームページ
各社の暗号化ハッシュ文書とSHV証明書
A社
B社
C社
暗号化ハッシュ文書
SHV証明書
101
S44
25
110
TTPホームページ（公開SHVデータ）
証明書ユーザID入力欄
1999 1/23 3:42:57 abcdef---
1999 1/23 3:42:58 AbCdEf---
1999 1/23 3:42:59 aBcDeF---
111
103a
103b
103c
27
S39
S40
S41
A社入札端末
B社入札端末
C社入札端末
11a
11b
11c

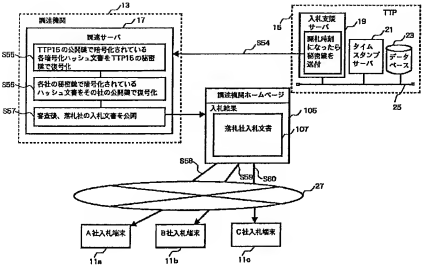
【図９】


13
調達機関
調達サーバ
17
16
TTP
S59
S61
S62
27
TTP15の公開鍵で暗号化
S48
S49
S60
A社暗号化ハッシュ文書に電子署名
S45
S46
S47
11a
11b
11c

【図１１】


検証開始
S61
図１０のステップS58、59、60でダウンロードした落札社入札文書107のハッシュをとって、開札後の入札文書のハッシュ値を生成する。
S62
落札社の秘密鍵による暗号化ハッシュ文書を落札社の公開鍵で復号化して、開札前の落札社入札文書のハッシュ値を得る。
S63
開札後のハッシュ値と開札前のハッシュ値とを比較し、一致していなければ、落札社の入札文書が開札後に改ざんされたと判断する。

【図１０】


13
調達機関
17
調達サーバ
S55
TTP15の公開鍵で暗号化されている各種符化ハッシュ文書をTTP15の秘密鍵で復号化
S56
各社の秘密鍵で暗号化されているハッシュ文書をその社の公開鍵で復号化
S57
落札社、落札社の入札文書を公開
15
TTP
入札支援サーバ
19
S54
落札社候になったら秘密鍵を送付
21
タイムスタンプサーバ
23
データベース
25
調達機関ホームページ
入札結果
105
落札社入札文書
107
S58
S59
S60
27
A社入札端末
11a
B社入札端末
11b
C社入札端末
11c

【図１２】

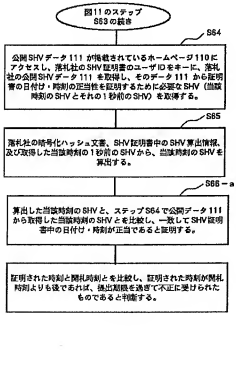
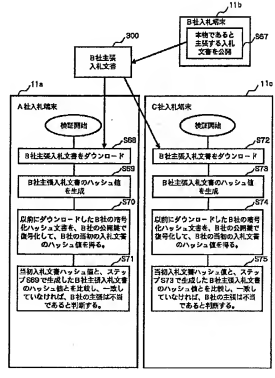


図11のステップS83の説明
S84
公開SHV データ111 が掲載されているホームページ110にアクセスし、落札社のSHV証明書のユーザIDをキーに、落札社の公開SHVデータ111 を取得し、そのデータ111 から証明書の日付け・時刻の正当性を証明するために必要なSHV（当該時刻のSHVとそれの１秒前のSHV）を取得する。
S85
落札社の暗号化ハッシュ文書、SHV証明書中のSHV算出情報、及び取得した当該時刻の１秒前のSHVから、当該時刻のSHVを算出する。
S86－a
算出した当該時刻のSHVと、ステップS84で公開データ111から取得した当該時刻のSHVとを比較し、一致してSHV証明書中の日付け・時刻が正当であると証明する。
証明された時刻と開札時刻とを比較し、証明された時刻が開札時刻よりも後であれば、後出期限を過ぎて不正に受けられたものであると判断する。

【図１３】


11b
B社入札端末
本物であると主張する入札文書を公開
S67
300
B社主張入札文書
11a
A社入札端末
検証開始
S68
B社主張入札文書をダウンロード
S69
B社主張入札文書のハッシュ値を生成
S70
以前にダウンロードしたB社の暗号化ハッシュ文書を、B社の公開鍵で復号化して、B社の当初の入札文書のハッシュ値を得る。
S71
当初入札文書ハッシュ値と、ステップS69で生成したB社主張入札文書のハッシュ値とを比較し、一致していなければ、B社の主張は不当であると判断する。
11c
C社入札端末
検証開始
S72
B社主張入札文書をダウンロード
S73
B社主張入札文書のハッシュ値を生成
S74
以前にダウンロードしたB社の暗号化ハッシュ文書を、B社の公開鍵で復号化して、B社の当初の入札文書のハッシュ値を得る。
S75
当初入札文書ハッシュ値と、ステップS73で生成したB社主張入札文書のハッシュ値とを比較し、一致していなければ、B社の主張は不当であると判断する。